CLAIMS:

1. A method for detecting when a device having a protection state is removed from a network with one of authorized and unauthorized removal, comprising the steps of:

at least once, setting the protection state to a predetermined state;

inserting the device having the set protection state into the network;

detecting a removal of the device from the network; and

responding by the device detecting a removal in accordance with the protection state of the device whose removal has been detected.

2. The method of claim 1, wherein said device is a consumer electronic device.

3. The method of claim 1, wherein the network is an in-home network.

4. The method of claim 1, further comprising the steps of:

on removal of the device from the network, performing the steps of-

optionally, first setting the protection state to unprotected, and then

removing the device from the network.

5. The method of claim 1, further comprising the steps of:

on reinsertion of the device into the network after a removal, performing the steps of-

optionally, first setting the protection state to protected or unprotected, and then

reinserting the device ~~into the~~ network.

6. The method of claim 1, wherein the predetermined state is one of protected and unprotected.

7. The method of claim 1, wherein said network is at least one of Bluetooth , wired Ethernet (IEEE std 802.3), wireless Ethernet (IEEE std 802.11a/b/g), Ultra Wide Band (IEEE std 802.15.3) and Zigbee (IEEE std 802.15.4).

8. The method of claim 1, wherein said responding step further comprises the steps of:

generating an alarm on the device that detects a removal, if the protection state of the device whose removal has been detected indicates the device is protected; and

optionally, generating an alert on the device that detects a removal, otherwise.

9. The method of claim 1, wherein said inserting step further comprises reinserting the device in the network after removal.

10. The method of claim 1, wherein said detecting step further comprises the step of transporting the protection state to one or more other devices in the network.

11. The method of claim 10, wherein said detecting step is performed by at least one of the device itself and at least one other device in the network.

12. The method of claim 11, wherein said device and said at least one other device is a consumer electronic device.

13. The method of claim 11, wherein said network is an in-home network.

14. The method of claim 12, wherein the predetermined state is one of protected and unprotected.

15. The method of claim 14, wherein said inserting step further comprises reinserting the device in the network after removal.

16. The method of claim 11, wherein said response is the steps of:

generating an alarm on the device that detects a removal, if the protection state of the device whose removal has been detected indicates the device is protected; and

optionally, generating an alert on the device that detects a removal, otherwise.

17. The method of claim 1, wherein said setting step further comprises the steps of:

providing a set/reset component for the protection state; and

setting said provided protection state by the set/reset component.

18. The method of claim 17, wherein said set/reset component is at least one of a button on the device, a physical key to be inserted/positioned in the device, an input received from another device over the network and a separate configuration device connected via a configuration link,

wherein, said configuration link is not part of said network and is capable of transferring the protection state to be set to the set/reset component.

19. The method of claim 17, wherein the physical key is a smartcard.

20. The method of claim 17, wherein the configuration device and configuration link is a CE remote control using an infrared point-to-point link, respectively.

21. The method of claim 17, wherein the configuration device and configuration link comprise an RF identification tag using a short range RF link, respectively.

22. A method for a device, maintaining a previous and current state for monitoring the protection state of a device in the network, to determine when to start and stop an alarm or alert, comprising the steps of:

setting the previous state to an alarm state and then repeatedly performing the steps of:

receiving the current protection state of a device in the network;

timing out after a predetermined number of attempts to perform the receiving step and then performing the steps of -

a. if the previous state is a protected state performing the steps of -

i. starting an alarm, and

ii. setting the previous state to an alarm-alert state;

b. if the previous state is not a protected state, optionally, performing the steps of -

iii. starting an alert, and

iv. setting the previous state to an alarm-alert state,

if the receiving step does not time out, performing the steps of -

c. if the previous state is an alarm state performing the steps of -

v. stopping one of the alarm and alert, and

vi. setting the previous state to the received current protection state.

23. The method of claim 1, wherein:

said protection state further comprises a previous and a current state; and

said responding step further comprises the method of claim 22.

24. The method of claim 16, wherein:

said protection state further comprises a previous and a current state; and

said responding step further comprises the method of claim 22.

25. A hardware/software system for a device connected to a network to detect one of authorized and unauthorized removal of a device from the network, comprising:

a settable protection state;

a transceiver for sending and receiving messages to and from other devices in the network;

an inspection control module configured to perform at least one of -

- detection of removal of the device itself or any other device from the network,

- detection of insertion of the device itself or any other device into the network,

- setting of the protection state,

- resetting of the protection state,

- generation of an alarm and, optionally, an alert, and

- cessation of an alarm and, optionally, an alert; and

output means for outputting said alarm and, optionally, means for outputting said alert, wherein said alert is generated if the system needs to generate such an alert.

26. The system of claim 25, further comprising a state set/reset component for setting/resetting the settable protection state.

27. The system of claim 26, wherein said state set/reset component is at least one of a button on the device, an input on a screen of the device, an input received via the transceiver from another network device, a physical key to be inserted/positioned in the device, a separate configuration device connected via a wired or wireless configuration link,
wherein, said configuration link is not part of said network and is capable of transferring the protection state to be set to the device.

28. The system of claim 27, wherein the physical key is a smartcard.

29. The system of claim 27, wherein the configuration device and configuration link is a CE remote control using an infrared point-to-point link, respectively.

30. The system of claim 27, wherein the configuration device and configuration link comprise an RF identification tag using a short range RF link, respectively.

31. The system of claim 25 wherein:

said protection state further comprises a previous and a current state; and

said output means is the method of claim 22; and

said alarm is at least one of a caii to the authorities, making the device unusable, a flashing light, a repetitive sound, and a message displayed on the device; and

said alert is at least one of a flashing light, a sound, and a message displayed on the device, wherein, said alarm and said alert are distinguishable by a user such that the alarm indicates an unauthorized removal and the alert indicates an authorized removal of the device from the network.